Ruby master - Bug #15162

Encoding::Converter.search_convpath(Encoding::ASCII_8BIT, Encoding::Emacs_Mule) crashes on MinGW

09/26/2018 09:35 AM - Eregon (Benoit Daloze)

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>ruby -v:</td>
<td>ruby 2.6.0dev (2018-09-26) [x64-mingw32]</td>
</tr>
<tr>
<td>Backport:</td>
<td>2.3: REQUIRED, 2.4: DONE, 2.5: DONE</td>
</tr>
</tbody>
</table>

Description

It seems to work fine with String arguments, but not Encoding objects where it SEGV, at least in some runs.
See [https://github.com/ruby/ruby/commit/f00bf242724d40d59a242c6bf9e567d18c9e1872#commitcomment-30650955](https://github.com/ruby/ruby/commit/f00bf242724d40d59a242c6bf9e567d18c9e1872#commitcomment-30650955)

cc MSP-Greg (Greg L)

Related issues:

Related to Ruby master - Bug #12411: Warnings when compiling transcode.c on c...

Closed

Associated revisions

Revision b965781e - 09/29/2018 06:47 AM - shirosaki
transcode.c: add GC guard on raise

- transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise. [Bug #15162] [ruby-core:89172]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64879 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 64879 - 09/29/2018 06:47 AM - shirosaki
transcode.c: add GC guard on raise

- transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise. [Bug #15162] [ruby-core:89172]

Revision 64879 - 09/29/2018 06:47 AM - shirosaki
transcode.c: add GC guard on raise

- transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise. [Bug #15162] [ruby-core:89172]

Revision e42dcdcb5 - 01/20/2019 10:48 AM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 64879: [Backport #15162]

transcode.c: add GC guard on raise

* transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise.
  [Bug #15162] [ruby-core:89172]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@66881 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 66881 - 01/20/2019 10:48 AM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 64879: [Backport #15162]

transcode.c: add GC guard on raise

* transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise.
  [Bug #15162] [ruby-core:89172]

Revision 673de310 - 01/31/2019 10:36 AM - usa (Usaku NAKAMURA)
merge revision(s) 64879: [Backport #15162]

03/07/2022
transcode.c: add GC guard on raise

* transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise.
  [Bug #15162] [ruby-core:89172]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@66961 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 66961 - 01/31/2019 10:36 AM - usa (Usaku NAKAMURA)
merge revision(s) 64879: [Backport #15162]

transcode.c: add GC guard on raise

* transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise.
  [Bug #15162] [ruby-core:89172]

History

#1 - 09/26/2018 11:42 AM - h.shirosaki (Hiroshi Shirosaki)
- File 0001-transcode.c-add-GC-guard-on-raise.patch added

I found a smaller test to reproduce SEGV.

$ ./miniruby -ve "loop do loop do loop do Encoding::Converter.search_convpath(Encoding::ASCII_8BIT, Encoding::ASCII_8BIT) end end end"
ruby 2.6.0dev (2018-09-26 trunk 64852) [x64-mingw32] Segmentation fault

Maybe GC guard is not sufficient? Attached patch fixes SEGV on my test.

#2 - 09/26/2018 11:29 PM - MSP-Greg (Greg L)
hsbt (Hiroshi SHIBATA), thanks for the work on this. I (quickly) did a lambda in a block, and that didn't cause the SEGV.

Using existing ruby-loco builds (I save all of them locally). I found that the issue doesn't exist on:
ruby 2.6.0dev (2018-09-26 trunk 64845) [x64-mingw32]
but does exist on:
ruby 2.6.0dev (2018-09-26 trunk 64851) [x64-mingw32]

I'll check the patch later, Greg

#3 - 09/27/2018 11:17 PM - MSP-Greg (Greg L)
hsbt (Hiroshi SHIBATA)

I just did twenty runs of core/encoding, then twenty runs of the full spec suite. No silent SEGV's.

Hence, the patch works. Thank you. Whoever does the commit, please remember to remove the two .name method calls on line 30 of spec/ruby/core/encoding/converter/search_convpath_spec.rb

Benoit - I can't seem to ping you using either Eregon (Benoit Daloze) or Eregon (Benoit Daloze)

#4 - 09/28/2018 12:24 AM - hsbt (Hiroshi SHIBATA)
MSP-Greg (Greg L)

You mistake to mention about @shirosaki, not @hsbt.

#5 - 09/28/2018 12:43 AM - MSP-Greg (Greg L)
hsbt (Hiroshi SHIBATA) & h.shirosaki (Hiroshi Shirosaki)

I apologize for that mistake. I hope to not make it again.

We have a saying something like 'foot in mouth' referring to speech. I'm not sure what the equivalent is for written... Thanks, Greg

#6 - 09/28/2018 09:16 AM - Eregon (Benoit Daloze)
MSP-Greg (Greg L) wrote:

Benoit - I can't seem to ping you using either Eregon (Benoit Daloze) or Eregon (Benoit Daloze)
Odd, not sure why it doesn't work.

#7 - 09/29/2018 06:25 AM - h.shirosaki (Hiroshi Shirosaki)
- Related to Bug #12411: Warnings when compiling transcode.c on cygwin added

#8 - 09/29/2018 06:46 AM - h.shirosaki (Hiroshi Shirosaki)
  Thank you for test.
  This issue seems to be related to #12411 fix.

#9 - 09/29/2018 06:47 AM - Anonymous
  - Status changed from Open to Closed

Applied in changeset trunk:r64879.

transcode.c: add GC guard on raise

  * transcode.c (econv_s_search_convpath): add GC guard to fix SEGV on raise. [Bug #15162] [ruby-core:89172]

#10 - 10/10/2018 10:51 AM - nagachika (Tomoyuki Chikanaga)
  - Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED

#11 - 01/20/2019 10:48 AM - nagachika (Tomoyuki Chikanaga)
  - Backport changed from 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE

ruby_2_5 r66881 merged revision(s) 64879.

#12 - 01/31/2019 10:36 AM - usa (Usaku NAKAMURA)
  - Backport changed from 2.3: REQUIRED, 2.4: DONE, 2.5: DONE to 2.3: REQUIRED, 2.4: DONE, 2.5: DONE

ruby_2_4 r66961 merged revision(s) 64879.

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-transcode.c-add-GC-guard-on-raise.patch</td>
<td>1.04 KB</td>
<td>09/26/2018</td>
<td>h.shirosaki (Hiroshi Shirosaki)</td>
</tr>
</tbody>
</table>